1-1994

On the equivalence of McEliece's and Niederreiter's public-key cryptosystems

Y. X. LI

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

X. M. WANG

DOI: https://doi.org/10.1109/18.272496

REFERENCES

[1] J. Ziv and A. Lempel, "Compression of individual sequences via variable-rate coding," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 530–536, Sept. 1978.

[2] J. Rissanen, "A universal data compression system," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 656–664, Sept. 1983.

[3] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

[4] P. Elias, "Universal codeword sets and representations of the integers," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 194–203, Mar. 1975.

[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[6] W. F. Stout, *Almost Sure Convergence*. New York: Academic, 1974.

[7] L. D. Davisson, "Universal noiseless coding," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 783–795, Nov. 1973.

[8] J. C. Kieffer, "A unified approach to weak universal source coding," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 674–682, Nov. 1978.

[9] A. D. Wyner, "An upper bound on the entropy series," *Inform. Contr.*, vol. 20, pp. 176–181, 1972.

[10] L. Györfi, I. Páli, and E. C. van der Meulen, "On universal noiseless source coding for infinite source alphabets," in *European Trans. Telecommun. Related Technol.*, vol. 4, pp. 125–132, Mar.–Apr. 1993.

On the Equivalence of McEliece's and Niederreiter's Public-Key Cryptosystems

Yuan Xing Li, *Member, IEEE*, Robert H. Deng, and Xin Mei Wang, *Member, IEEE*

***Abstract*—It is shown that McEliece's and Niederreiter's public-key cryptosystems are equivalent when set up for corresponding choices of parameters. A security analysis for the two systems, based on this equivalence observation, is presented.**

***Index Terms*—Cryptosystems, McEliece's cryptosystem, Niederreiter's cryptosystem, security, algebraic codes.**

I. INTRODUCTION

Since the concept of public-key cryptosystems appeared in the fundamental paper of Diffie and Hellman [1] in 1977, the field of cryptology has undergone a dramatic development. The last decade has seen explosive growth in unclassified research in all aspects of cryptology. Public-key cryptosystem and cryptanalysis have been two of the most active areas. So far many kinds of public-key cryptosystems have been proposed, and many of them that had been thought to be secure have been broken.

A special class of public-key cryptosystems were constructed based on algebraic error-correcting codes. In the present paper, we focus on two such systems, McEliece's [2] and Niederreiter's [3] cryptosystems, examine the relationship between the two, and derive the interesting result that the two systems are equivalent and have the same security when set up for corresponding choices of parameters. This result allows us to clarify the security evaluations of Niederreiter's cryptosystem, by Niederreiter [3] and by Brickell and Odlyzko [4]. Furthermore, we employ the best known attack, the Lee–Brickell attack [5], to cryptanalyze the two systems. Some new optimal parameter values and work factors are obtained.

We briefly review McEliece's and Niederreiter's cryptosystems in Section II. The equivalence of the two systems is derived in Section III. Finally, we cryptanalyze the two systems and comment on the selection of optimal system parameters in Section IV.

Manuscript received May 4, 1993; revised November 17, 1993. This work was supported in part by the National Natural Science Foundation of China under Grant 69072910.

Y. X. Li is with the Magnetic Technology Centre, National University of Singapore, Kent Ridge, Singapore 0511, Republic of Singapore.

R. H. Deng is with the Department of Electrical Engineering, National University of Singapore, Kent Ridge, Singapore 0511, Republic of Singapore.

X. M. Wang is with the Department of Information Engineering, Xidian University, People's Republic of China.

IEEE Log Number 9215123.

II. MCELIECE'S AND NIEDERREITER'S CRYPTOSYSTEMS

In this section, brief descriptions of McEliece's and Niederreiter's cryptosystems are presented in order to facilitate discussions in later sections. Both cryptosystems are algebraic-coded two-key systems. The basic idea behind them was to construct a linear error-correcting code for which a fast decoding algorithm is known, and then to disguise it as a general linear code whose decoding problem is NP-complete.

A. McEliece's Cryptosystem [2]

This system uses a binary $(n, k, 2t+1)$ Goppa code C where n is the code length, k is the code dimension, and t is the error-correcting capability of C. C is constructed by randomly selecting an irreducible polynomial of degree t over GF(2^l) as the Goppa polynomial (note that $n = 2^l$). Let $\boldsymbol{G}$ be a $k \times n$ generator matrix of C [6], $\boldsymbol{S}$ any $k \times k$ nonsingular matrix, and $\boldsymbol{P}$ any $n \times n$ permutation matrix.

- Private Key: $\boldsymbol{G}$, $\boldsymbol{S}$, $\boldsymbol{P}$.
- Public Key: $\boldsymbol{G'} = \boldsymbol{SGP}$ and t.
- Messages: k bit vectors $\boldsymbol{m}$ over GF(2).
- Encryption: $\boldsymbol{c} = \boldsymbol{mG'} + \boldsymbol{e}$. $\boldsymbol{e}$, an n bit error vector with (Hamming) weight t. $\boldsymbol{c}$, the n bit ciphertext.
- Decryption: Since $\boldsymbol{c} = \boldsymbol{mSGP} + \boldsymbol{e}, \boldsymbol{cP^{-1}} = (\boldsymbol{mS})\boldsymbol{G} + \boldsymbol{eP^{-1}}$. Use a fast decoding algorithm for C to correct the error "$\boldsymbol{eP^{-1}}$, find $\boldsymbol{mS}$ and thus $\boldsymbol{m}$.

McEliece investigated several attacks against his system. One of those was to factor the public key to obtain the private key, but this approach was thought to be hopeless. Another attack, considered as the most promising, was to pick k "error-free" elements of the ciphertext $\boldsymbol{c}$, and then to solve a set of $\boldsymbol{k}$ linear equations to recover the message $\boldsymbol{m}$. Using this attack, McEliece suggested using $n = 1024$ and $t = 50$, i.e., (1024, 524, 101) Goppa code in his system. The corresponding work factor of the system is approximately $2^{80.7}$ [7].

B. Nederreiter's Cryptosystem [3]

This is a knapsack-type cryptosystem which employs an $(n, k, 2t+1)$ linear code C over GF(q). Let $\boldsymbol{H}$ be an $(n-k) \times n$ parity check matrix of C, $\boldsymbol{M}$ any $(n-k) \times (n-k)$ nonsingular matrix, and $\boldsymbol{P}$ any $n \times n$ permutation matrix, all over GF(q).

- Private Key: $\boldsymbol{H}$, $\boldsymbol{M}$, and $\boldsymbol{P}$.
- Public Key: $\boldsymbol{H'} = \boldsymbol{MHP}$ and t.
- Messages: n dimensional vectors $\boldsymbol{y}$ over GF(q) with weight t.
- Encryption: $\boldsymbol{z} = \boldsymbol{yH'^T}$. $\boldsymbol{z}$, the ciphertext of dimension $n-k$.
- Decryption: Since $\boldsymbol{z} = \boldsymbol{y}(\boldsymbol{MHP})^{\boldsymbol{T}}, \boldsymbol{z}(\boldsymbol{M^T})^{-1} = (\boldsymbol{yP}^T)\boldsymbol{H^T}$. Use a fast decoding algorithm for C to find $\boldsymbol{yP^T}$ and thus $\boldsymbol{y}$.

Niederreiter [3] cryptanalyzed his system and mentioned two example systems, one using a binary concatenated (104, 24, 31) code and the other using a (30, 12, 19) Reed–Solomon code over GF(31). The examples were later verified as insecure by Brickell and Odlyzko

[4]. The attack used in Niederreiter's cryptanalysis was to factorize H' in the hope of getting M, H, and P. However, this cryptanalysis was not sufficient to ensure the security of his cryptosystem. Actually, McEliece has shown that this attack was not the most threatening.

In the following, we derive the equivalence relationship between the two cryptosystems, and re-evaluate the securities of the two systems using the best known attack, the Lee–Brickell attack.

III. Equivalence of the McEliece's and Niederreiter's Cryptosystems

A fair comparison of the two systems dictates that they both be based on the same error-correcting $(n, k, 2t+1)$ linear code C. Let H and G denote the parity check matrix and the generator matrix, respectively, of C. Then finding H from G (or equivalently finding G from H) can be achieved by linear algebra [6]. For instance, by converting the generator matrix into the systematic form $G = [I_k A]$, the parity check matrix is simply given by $H = -[A^T I_{n-k}]$.

Given the public key G' and the encryption equation $c = mG' + e$ in McEliece's cryptosystem, multiplying both sides of the equation by H'^T, we obtain

$$z \equiv cH'^T = mG'H'^T + eH'^T = eH'^T \tag{1}$$

since $G'H'^T = 0$. Note that (1) is identical to Niederreiter's encryption equation. Given z and H', if e can be found, i.e., Niederreiter's cryptosystem is broken, so is McEliece's cryptosystem. Therefore, it is not more difficult to break McEliece's cryptosystem than to break Niederreiter's cryptosystem.

On the other hand, given the public key H' and the encryption equation $z = yH'^T$ in Niederreiter's cryptosystem, by linear algebra, an $n-$dimensional vector c of weight larger than or equal to t can be found such that $z = cH'^T$. Obviously, c may be expressed as

$$c = mG' + y \tag{2}$$

where m is a $k-$dimensional vector and the weight of y is t. Equation (2) is just (2) McEliece's encryption equation. Therefore, if McEliece's cryptosystem can be broken, so can Niederreiter's cryptosystem.

IV. Security Comments

McEliece [2] suggested two possible attacks on his cryptosystem. The first attack is to factor the public key G' in the hope of finding the private key S, G, and P, i.e., finding trapdoors to his system. Adams and Meijer [7] stated that there is usually only one trapdoor in McEliece's cryptosystem. Recently, Gibson [8] showed that there always exist multiple trapdoors in any instance of McEliece's system. However, it seems difficult to find trapdoors to McEliece's system. The second attack proposed by McEliece is to directly recover m from c without using the private key. The basic idea of this attack is to repeatedly select k bits at random from an $n-$bit ciphertext vector and estimate m based on the k selected bits. If the k selected bits are error-free, the message m will be recovered; otherwise, the process is repeated by selecting another set of k bits from c until the message is recovered correctly.

The best known attack, proposed by Lee and Brickell [5], is a generalization of McEliece's second attack. The Lee–Brickell attack allows the k selected bits to contain some errors, and try to recover the message correctly. Because of the equivalence of McEliece's and Niedereiter's cryptosystems, in the following we will cryptanalyze McEliece's cryptosystem under the best known attack. The results of the analysis apply equally well to Niederreiter's cryptosystem, provided that the two cryptosystems are based on the same error-correcting code. Without loss of generality, we assume, throughout the rest of the paper, that the same binary error-correcting codes are used in the two systems.

Attack 1 (Lee–Brickll Attack): Picke a $k \times k$ submatrix G'_k of G' consisting of the j_1th, j_2th, $\cdots$, and the j_kth columns of G'. Let c_k and e_k be the k dimensional vectors consisting of the j_1th, j_2th, $\cdots$, and the j_kth bits of c and e, respectively. It then follows that $c_k + e_k = mG'_k$ and that $(c_k + e_k)(G'_k)^{-1}G = mG'_k(G'_k)^{-1}G = mG$. Choose a k-bit vector e'_k with $j(\leq t)$ or fewer ones. If $c + (c_k + e'_k)(G'^{-1}_k)G$ has weight t, then $e'_k = e_k$ and the message $m = (c_k + e'_k)(G'_k)^{-1}$ is recovered; otherwise, choose another e'_k and repeat the above process. If all the k bit error patterns e'_k of weight $\leq j$ have been exhausted and the message still can not be recovered, then pick another submatrix of G' and the above process is repeated. The process continues until m is found.

The probability that there are i errors in the randomly chosen $k-$bit vector c_k is

$$p_i = \binom{t}{i}\binom{n-t}{k-i}\Big/\binom{n}{k}$$

Therefore, the probability that the attack completes successfully is $\sum_{i=0}^{j} p_i$ and that the average number of times we must repeat the algorithm before we are successful is

$$T_j = 1/\sum_{i=0}^{j} p_i. \tag{3}$$

The number of k bit error patterns with j or fewer ones is

$$N_j = \sum_{i=0}^{j}\binom{k}{i}.$$

Thus, the average overall work factor for this attack is

$$W1_j = T_j(\alpha k^3 + N_j \beta k). \tag{4}$$

Attack 1 is based on the encryption equation $c = mG' + e$. As we have previously shown, this equation can be transformed into the encryption equation $z = eH'^T$ by linear algebra. Therefore, the security of McEliece's cryptosystem may also be analyzed using a Lee–Brickell type attack based on $z = eH'^T$. This is demonstrated below.

Attack 2: Pick an $(n-k) \times (n-k)$ submatrix H'_{n-k} of H' consisting of the j_1th, j_2th, $\cdots$, j_{n-k}th columns of H'. Let e_{n-k} be the $(n-k)$ bit vector consisting of the j_1th, j_2th, $\cdots$, j_{n-k}th bits of e. Let $e_n(n-k)$ be the n bit vector which is identical to e_{n-k} in positions $j_1, j_2, \cdots, j_{n-k}$, and with the other k positions set to zero. Furthermore let $e_n(k) = e + e_n(n-k)$. Then $z = eH'^T = (e_n(n-k) + e_n(k))H'^T = e_n(n-k)H'^T + e_n(k)H'^T$. Multiply both sides of the above equation by $(H'^T_{n-k})^{-1}$, and after rearrangement, we have $e_{n-k} = (z + e_n(k)H'^T)(H'^T_{n-k})^{-1}$. Choose an n-bit vector $e'_n(k)$ with $(n-k)$ zeros at positions $j_1, j_2, \cdots, j_{n-k}$, and $j(\leq t)$ or fewer ones at the other k positions. Calculate $e'_{n-k} \equiv (z + e'_n(k)H'^T)(H'^T_{n-k})^{-1}$. Augment e'_{n-k} into an n bit vector $e'_n(n-k)$ which is identical to e'_{n-k} in positions $j_1, j_2, \cdots, j_{n-k}$, and with the other k positions set to zero. If $e'_n(n-k) + e'_n(k)$ has weight t and $(e'_n(n-k) + e'_n(k))H'^T = z$, then $e = e'_n(n-k) + e'_n(k)$ is found; otherwise, choose another $e'_n(k)$ and repeat the above procedure. If all the possible vectors $e'_n(k)$ have been tried and e still cannot be found, pick another H'_{n-k} and repeat the above process. The process continues until e is recovered.

The probability that there are $t-i$ ones among the randomly chosen $(n-k)$ bit vector $\boldsymbol{e}_{n-k}$ is

$$p_i = \binom{t}{t-i}\binom{n-t}{n-k-t+i}\Big/\binom{n}{n-k} = \binom{t}{i}\binom{n-t}{k-i}\Big/\binom{n}{k}. \quad (5)$$

Therefore the probability that the algorithm finishes successfully is $\sum_{i=0}^{j} p_i$. The average number of executions T_j is then again given by (3) with p_i's given in (5). The number of all possible n bit error patterns $\boldsymbol{e}'_n(k)$ is

$$N_j = \sum_{i=0}^{j}\binom{n}{i}.$$

Consequently, the average overall work factor for attack 2 is

$$W2_j = T_j(\alpha(n-k)^3 + N_j\beta(n-k)). \quad (6)$$

With $\alpha = \beta$, Lee and Brickell showed that the optimum j which minimizes the work factor $W1_j$ is 2 for all values of useful code parameters. This conclusion also applies to $W2_j$. Assuming $\alpha = \beta = 1$ and $n = 1024$, they further showed that the value of t which maximizes $W1_2$ is 38 and that $W1_2 \approx 2^{73.4}$. This result represents a reduction of order 2^{11} as compared with the work factor obtained by Adams and Meijer [7].

With Attacks 1 and 2 presented above, the work factor of attacking McEliece's–Nederreiter's cryptosystem should be defined as

$$W = \min\{W1_2, W2_2\} \quad (7)$$

and the coding parameters should be selected to maximize W. Again assuming $\alpha = \beta = 1$ and $n = 1024$, our calculations showed that the value of t which maximizes (7) is 41. With this new optimum value of $t, W1_2 \approx 2^{73.1}, W2_2 \approx 2^{71.9}$, and therefore, $W = W2_2 \approx 2^{71.9}$. Note that, although $t = 38$ maximizes $W1_2$, it does not maximizes W, since in this case $W2_2 \approx 2^{71.8}$.

Brickell and Odlyzko [4] proposed another attack on McEliece's cryptosystem based on the low density algorithm of [9]. However, the lattice basis reduction algorithm employed in this attack is not guaranteed to find the vector $\boldsymbol{e}$, and the attack does not seem promising.

It should be mentioned that Korzhik and Turkin [10] claimed to have found a polynomial time algorithm for decoding linear codes up to their minimum distance, which in particular would allow one to break the two cryptosystems discussed in this paper. However, since the description of this algorithm is very complicated and its correct functioning within the claimed time bounds could never be confirmed experimentally according to the authors' information, it appears doubtful whether this attack has any real significance.

ACKNOWLEDGMENT

The authors would like to express their deep gratitude to Prof. U. M. Maurer, the Institute for Theoretical Computer Science, Switzerland, for his valuable advice and comments which have helped improve the quality and the presentation of the paper significantly. The authors are also grateful to the referees for their helpful comments.

REFERENCES

[1] W. Diffie and M. E. Hellman, "New direction in cryptography," *IEEE Trans. Inform. Theory,* vol. IT-22, pp. 644–654, Nov. 1976.
[2] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *DSN Prog. Rep.,* Jet Prop. Lab., California Inst. Technol., Pasadena, CA, Jan.–Feb. 1987, pp. 114–116.
[3] H. Niederreiter, "Knapsack-tye cryptosystems and algebraic coding theory," *Prob. Contr. Inform. Theory,* vol. 15, no. 2, pp. 157–166, 1986.
[4] E. F. Brickell and A. M. Odlyzko, "Cryptanalysis: A survey of recent results," *Proc. IEEE,* vol. 76, pp. 578–593, May, 1988.
[5] P. J. Lee and E. F. Brickell, "An observation on the security of McEliece's public-key cryptosystem," in *Advance in Cryptology: Proc. Eurcrypto '88.* New York: Springer-Verlag, 1989, pp. 275–280.
[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1977.
[7] C. M. Adams and H. Meijer, "Security-related comments regarding McEliece's public-key cryptosystem," *IEEE Trans. Inform. Theory,* vol. 35, pp. 454–455, Apr. 1989.
[8] J. K. Gibson, "Equivalent Goppa codes and trapdoors to McELiece's public-key cryptosystem," in *Advance in Cryptology: Proc. Eurcrypto '91.* New York: Springer-Verlag, 1992, pp. 517–521.
[9] J. C. Kagarias and A. M. Odlyzko, "Solving low density subset sum problems," *J. Assoc. Comput.,* vol. 32, pp. 229–246, Mar. 1985.
[10] V. I. Korzkik and A. I. Turkin, "Cryptanalysis of McEliece's public-key cryptosystem," in *Advance in Cryptology: Proc. Eurcrypto '91.* New York: Springer-Verlag, 1992, pp. 27–28.

An Attack on the *Interlock Protocol* When Used for Authentication

Steven M. Bellovin and Michael Merritt

***Abstract*—Exponential key exchange may be used to establish secure communications between two parties who do not share a private key. It fails in the presence of an active wiretap, however. Davies and Price suggest the use of Shamir and Rivest's "Interlock Protocol" to surmount this difficulty. We demonstrate that an active attacker can, at the cost of a timeout alarm, bypass the passwork exchange, and capture the passwords used. Furthermore, if the attack is from a terminal or workstation attempting to contact a computer, the attacker will have access before any alarm can be sounded.**

***Index Terms*—Cryptography, protocol, security, authentication, exponential key exchange, Diffie–Hellman**

I. INTRODUCTION

The exponential key exchange protocol [1] has been suggested as a form of public-key cryptosystem. It is also useful if two parties wish to set up a secret conversation without prior arrangement, as the public keys are relatively easy to generate.

The dialog works as follows. Let α and β be large, publicly known numbers. Suppose that A wishes to talk privately with B. Each side picks a random number, A_R and B_R. The following messages are sent:

$$\boxed{A} \qquad\qquad \boxed{B}$$
$$\alpha^{A_R} \bmod \beta \;\rightarrow$$
$$\leftarrow \quad \alpha^{B_R} \bmod \beta.$$

At this point, A, who knows A_R, can calculate

$$(\alpha^{B_R})^{A_R} \bmod \beta \equiv \alpha^{A_R B_R} \bmod \beta.$$

Manuscript received July 15, 1990; revised January 31, 1993.
The authors are with AT&T Bell Laboratories, Murray Hill, NJ 07974.
IEEE Log Number 9215185.